拡張Hensel構成を用いた多変数多項式の因数分解の効率性

AUTHOR(S):

稲葉, 大樹

CITATION:

稲葉, 大樹. 拡張Hensel構成を用いた多変数多項式の因数分解の効率性. 数理解析研究所講究録 2005, 1456: 10-17

ISSUE DATE:

2005-11

URL:

http://hdl.handle.net/2433/47839

数理解析研究所講究録 1456 巻 2005 年 10-17

10

拡張Hensel構成を用いた多変数多項式の因数分解の効率性

稲葉 大樹

DAIJU INABA

筑波大学 数理物質科学研究科 数学専攻

DOCTORAL PROGRAM IN MATHEMATICS, UNIVERSITY OF TSUKUBA *

Abstract

拡張 Hensel 構成とは、展開点が特異点で非零代入を行わない Hensel 構成である。本稿では主係数問題への対応を行った拡張 Hensel 構成を用いた多変数多項式の因数分解法を計算機に実装し、一般 Hensel 構成において非零代入により項数増大が起こる多変数多項式の因数分解が効率良く行えるかどうかを検証する。

1 はじめに

$\mathbf{K}$ を数体とし、$F(x,u_1,\ldots,u_\ell)$ を $\mathbf{K}$ 上の無平方である多項式とし、$\bar{\mathbf{K}}$ を $\mathbf{K}$ の代数的閉包とする。また、$(s_1,\ldots,s_\ell)$ を Hensel 構成の展開点とする。

一般 Hensel 構成において $F(x,s_1,\ldots,s_\ell)$ が無平方でない場合、$(s_1,\ldots,s_\ell)$ を Hensel 構成の特異点といい、$F(x,u_1,\ldots,u_\ell)$ の主係数が $(s_1,\ldots,s_\ell)$ で 0 になるとき、$(s_1,\ldots,s_\ell)$ で主係数が特異であるという。

多変数多項式の一般 Hensel 構成の主な応用の一つとして多変数多項式の因数分解が挙げられる。基本的に展開点を原点として Hensel 構成を行うことにより、因数分解に必要な Hensel 因子が得られる。

しかし、原点が特異点もしくは原点で主係数が特異である場合、一般 Hensel 構成は破綻する。このとき、展開点を変更する必要がある。実際の計算では展開点により多項式の平行移動を行う (これを非零代入という) が、多項式によってはこれを行うことにより平行移動後の多項式の項数が爆発的に増加する場合があり、これにより Hensel 構成に時間がかかってしまう。これを非零代入問題という ([GCL92] では *bad-zero problem* と表記)。

展開点が特異点である場合の Hensel 構成について 2 変数多項式に対しては 1989 年に Kuo により [Kuo89]、多変数多項式に対しては 1993 年に Sasaki と Kako により [SK99]、考案された。この方法を Sasaki と Kako は拡張 Hensel 構成と命名した。さらに、Sasaki と Inaba は主係数が特異である場合にも適用できるように Sasaki-Kako の方法を拡張し、拡張 Hensel 構成を用いた多変数多項式の因数分解の方法も提案した ([SI00] 参照)。

[Ina04] において、多項式の主係数を初期因子に適切に振り分けることにより、拡張 Hensel 構成における多変数多項式の因数分解アルゴリズムを実装した。しかし、これだけでは効率化できる多項式が科なり限られる。そこで本稿ではさらなる工夫をすることにより、より広範囲の多項式に対して効率化できるできるようにしたい。

本稿では 2 章で拡張 Hensel 構成とそれを構成を用いた因数分解法の概要 (詳細は [SK99], [SI00] を参照されたい) を紹介し、3 章では [Ina04] で述べた因数分解アルゴリズムをさらに効率化させるための工夫法を紹介する。4 章では拡張 Hensel 構成を用いた多変数多項式の因数分解法を実装し、その効率性を従来の一般 Hensel 構成を用いた方法と比較、検証する。

2 拡張Hensel構成を用いた因数分解

$\mathbf{K}$ を数体とし、$\bar{\mathbf{K}}$ を $\mathbf{K}$ の代数的閉包とする。$\mathbf{K}[u_1,\ldots,u_\ell]$, $\mathbf{K}(u_1,\ldots,u_\ell)$ と $\mathbf{K}\{u_1,\ldots,u_\ell\}$ をそれぞれ $\mathbf{K}$ 上 $u_1,\ldots,u_\ell$ を変数とする多項式環、有理式体、形式的べき級数環とする。$(s_1,\ldots,s_\ell)\in\bar{\mathbf{K}}^\ell$ とし、$(u_1,\ldots,u_\ell)$ と $(s_1,\ldots,s_\ell)$ をそれぞれ (u) と (s) と略記する。多項式 $F(x,u)\in\mathbf{K}[x,u]$ は無平方 (重複因子が存在しない) で各変数について原始的 (係数が互いに素) であるとし、

$$F(x,u)=f_n(u)x^n+f_{n-1}(u)x^{n-1}+\cdots+f_0(u)x^0,\quad f_n(u)\neq 0 \tag{1}$$

*inaba@math.tsukuba.ac.jp

と表記する。$\deg(F)$, $\mathrm{lc}(F)$ をそれぞれ多項式 F の x に関する次数、主係数とする。$\mathrm{tdeg}(f_i)$ を各 f_i の $u_1,\ldots,u_\ell$ に関する全次数 (f_i の各項 $T = cu_1^{e_1}\cdots u_\ell^{e_\ell}$ $(c\neq 0)$ に対し、その全次数 $\mathrm{tdeg}(T) = e_1+\cdots+e_\ell$ の最大をとる) とする。$\mathrm{ord}(f_i)$ を f_i の各項の全次数のうち最小のものとし、これを f_i の位数という。また、有理関数 $f(u)/g(u)$ に関して、その位数を $\mathrm{ord}(f/g) = \mathrm{ord}(f) - \mathrm{ord}(g)$ で定義する。$\gcd(F,G)$ を多項式 F と G の最大公約数とし、$\mathrm{cont}(F) = \gcd(f_n, f_{n-1},\cdots,f_0)$ を $F(x,u)$ の係因数とする。

u の有理式 $G(u)$ が以下のように分解されるものとする。

$$\begin{cases} G(u) = g_0(u)/d_0(u) + g_1(u)/d_1(u) + \cdots + g_k(u)/d_k(u) + \cdots \\ \qquad g_k(u) \text{ と } d_k(u) \text{ は } \bar{\mathbf{K}}[u] \text{ に関して同次式} \\ \qquad \mathrm{ord}(g_k/d_k) = k \quad (k = 0,1,2,\ldots) \end{cases} \tag{2}$$

$\bar{\mathbf{K}}\{(u)\}$ を (2) のような負でない位数から成る同次有理式の級数環とする。

定義 1 (特異点、主係数が特異)
展開点 (s) に対し、$F(x,s)$ が無平方でないとき、(s) を (Hensel 構成の) 特異点という。また、$f_n(s)=0$ をみたすとき、(s) で主係数が特異であるという。

まず、従変数 $u_1,\ldots,u_\ell$ の全次数変数 t を $u_i \mapsto tu_i$ $(i=1,\ldots,\ell)$ という変換で導入する。(または、$u_i \mapsto t^{\omega_i}u_i$ $(i=1,\ldots,\ell)$、$(\omega_1,\ldots,\omega_\ell$ は正の数) と、重みをつけて導入してもよい。) 全次数変数導入後の多項式を $\hat{F}(x,t,u)$ とする。

定義 2 ($F(x,u)$ の Newton 線 $\mathcal{L}$ と Newton 多項式 $F_{\mathrm{New}}(x,u)$)
0 でない $\hat{F}(x,t,u)$ の各項 $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}$ $(c\in\mathbf{K},\ j=j_1+\cdots+j_\ell)$ に対応する点 (i,j) を (e_x,e_t)-平面にプロットする。$\nu=\mathrm{ord}(f_n)$ とし、点 (n,ν) (図 1 では点 P を指す) を通る (e_x,e_t)-平面上の直線のうち、他の少なくとも一点を通り、直線より下にはプロットが存在しないものを $F(x,u)$ の Newton 線 ($\mathcal{L}$ と表記) と定義する。$\mathcal{L}_{\mathrm{New}}$ 上にあるプロットに対応する全ての項の和を $F(x,u)$ の Newton 多項式 ($F_{\mathrm{New}}(x,u)$ と表記) と定義する。

例 1
以下の多項式 F を考える。

$$\begin{aligned} F(x,y,z) = {} & x^4(y^2-z^2) + x^3(y+3z+3y^2+3z^2) \\ & + x^2(-2+3y-4z-2y^2+5yz-2z^2+y^3+6y^2z+3z^3) \\ & + x^1(-5y-9y^2-5yz-5z^2+3y^3+y^2z-5z^3) \\ & + (3y^2-5y^3-7y^2z-yz^2-2y^4-3y^2z^2-3yz^3-2z^4). \end{aligned}$$

$F(x,y,z)$ の各項のプロットは右図で、Newton 多項式 $F_{\mathrm{New}}(x,y,z)$ は下式となる。

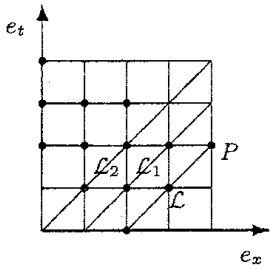

図 1

$$\begin{aligned} F_{\mathrm{New}} &= x^4(y^2-z^2) + x^3(y+3z) - 2x^2 \\ &= x^2\cdot[x(y-z)+2]\cdot[x(y+z)-1]. \quad \square \end{aligned}$$

F_{New} を互いに素な因子 $G_1^{(0)},\ldots,G_r^{(0)}$ に分解し、これらの因子を初期因子として

$$F(x,u) \equiv G_1^{(k)}(x,u)\cdots G_r^{(k)}(x,u) \pmod{I_{k+1}}. \tag{3}$$

となるように分解するのが拡張 Hensel 構成である。ここでイデアル I_k は上記で $k=0\Rightarrow 1\Rightarrow 2\Rightarrow\cdots$ と上げていくとき、新たに取り込まれる項を通る直線 $\mathcal{L}_k$ が $\mathcal{L}$ に平行のまま上にシフトし、かつ全てのプロット点を走査するように決める。

定義 3 ($G(x,u)$ の Newton 多角形)
$G(x,u)\in\bar{\mathbf{K}}\{(u)\}[x]$ において $G(x,tu)$ の各項 $cx^it^ju_1^{j_1}\cdots u_\ell^{j_\ell}/D(tu)$ $(c\in\bar{\mathbf{K}},\ j=j_1+\cdots+j_\ell,\ D(u)$ は $\mathrm{ord}(D)=d$ を満たす $u_1,\ldots,u_\ell$ についての同次多項式) に対応する点 $(i,\ j-d)$ を (e_x,e_t)-平面にプロットする。このとき、$G(x,u)$ の Newton 多角形 $\mathcal{N}$ はプロットされた全ての点に対する凸包と定義する。さらに $\mathcal{N}$ の下辺を時計回りに $\mathcal{S}_1,\ldots,\mathcal{S}_\rho$ とする。

Newton 線は最右側の下辺である $\mathcal{S}_1$ に過ぎない。図 2 は例 1 の多項式における Newton 多角形で、この場合図 2 の $\mathcal{S}_1, \mathcal{S}_2$ が下辺である。
Newton 多角形の下辺が 1 本、つまり $\rho = 1$ であるとき、拡張 Hensel 構成は 1 回で済む。この場合は一般 Hensel 構成と同様に Hensel 因子に分解できる。以下、$\rho > 1$ の場合について述べる。まず、$F(x,u)$ の Newton 多項式 $F_{\mathcal{S}_1}$ を以下の通りに分解する (下記の n_1 は $F_{\mathcal{S}_1}$ の最小次数)。

$$F_{\mathcal{S}_1} = x^{n_1} \cdot \mathrm{cont}(F_{\mathcal{S}_1}) G_1^{(0)}(x,u) \cdots G_r^{(0)}(x,u). \tag{4}$$

ただし、$x^{n_1}, G_1^{(0)}, \ldots, G_r^{(0)}$ は互いに素であるとする。これらを初期因子として拡張 Hensel 構成を行うと $F(x,u)$ は以下の通りに分解できる。

$$F(x,u) = F_2(x,u) \cdot \mathrm{cont}(F_{\mathcal{S}_1}) G_1^{(\infty)}(x,u) \cdots G_r^{(\infty)}(x,u). \tag{5}$$

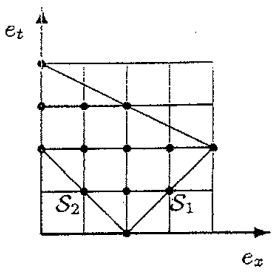

図 2：Newton 多角形の例

ここで、$F_2(x,u)$ は x^{n_1} に対応する Hensel 因子であるが、この $F_2(x,u)$ に再び拡張 Hensel 構成を適用する (Newton 線は $\mathcal{S}_2$) ことで Hensel 因子に分解できる。以上を繰り返すことにより、$\mathcal{S}_1 \Rightarrow \mathcal{S}_2 \Rightarrow \cdots \Rightarrow \mathcal{S}_\rho$ の順に Hensel 因子を得ることができる。ただし、得られる Hensel 因子は [SI00] の Theorem 1 (分解定理) より $\bar{\mathbf{K}}\{u\}[x]$ ではなく $\bar{\mathbf{K}}\{(u)\}[x]$ 内の式になる。
次に因子の組み合わせについて述べる。まず $\bar{\mathbf{K}}\{(u)\}[x]$ 内のいくつかの既約因子をかけることで $\bar{\mathbf{K}}\{u\}[x]$ 内の既約因子を作るが、これは以下の方法で行う。

1. まず、各 $i \in \{1, \ldots, \rho\}$ に対し、$\mathcal{S}_i$ 上に対応する Hensel 因子同士で固有の分母因子 $d_i(u)$ を持つとき、それらを組み合わせて分母 $d_i(u)$ を消去する (この方法は拡張 Hensel 構成の計算途中で行うことができる)。
2. 次に $\mathcal{S}_1, \ldots, \mathcal{S}_\rho$ 内で異なる辺上の Hensel 因子が固有の分母因子を持てば、それらを組み合わせてその分母を消去する。

上記の組み合わせが終了した後、生成した $\bar{\mathbf{K}}\{u\}[x]$ 内のいくつかの既約因子をかけることで $\bar{\mathbf{K}}[x,u]$ 内の既約因子を作る。

3 拡張 Hensel 構成における因数分解の効率化への工夫

3.1 有理 Hensel 因子の組合せ

多変数多項式の拡張 Hensel 構成における Hensel 因子は一般には有理式で表される。しかし、有理 Hensel 因子どうしの計算は大変時間がかかる。もし、有理 Hensel 因子どうしを組合せてべき級数 Hensel 因子が生成できれば大幅に効率化されるであろう。そのためには同じ分母因子をもつ Hensel 因子同士で組み合わせることで、べき級数 Hensel 因子を作りだすことができる。

例 2

$$\begin{aligned} F \;=\; & x^5 + x^4(-10y - z) \\ & + x^3(3y^2 + 16yz - 2z^2 - 5y^3z^3) \\ & + x^2(-27y^2z + 8yz^2 + 126y^3 + 4y^3z^3 - 63y^4z^3 + 19y^3z^4) \\ & + x(-252y^3z + 42y^2z^2 + 12y^4z^3 - 8y^3z^4 + 126y^5z^3 + 27y^4z^4 - 24y^6z^6) \\ & + (-24y^4z^4 + 12y^6z^6). \end{aligned}$$

F の Newton 多角形について、下辺は 1 本のみである。従って、拡張 Hensel 構成は 1 回のみでよい。
Newton 多項式 F_{New} の既約分解は以下の通りである。

$$F_{\mathrm{New}} = x(x+3y)(x-6y+z)(x-7y)(x-2z).$$

$G_1 = x$, $G_2 = x + 3y$, $G_3 = x - 6y + z$, $G_4 = x - 7y$, $G_5 = x - 2z$ とし、拡張 Hensel 構成を適用する。3 次まで行

うと以下の *Hensel* 因子を得る。

$$\begin{aligned} G_1^{(3)} &= x + \frac{4y^2z^3}{7(6y-z)}, \\ G_2^{(3)} &= x + 3y, \\ G_3^{(3)} &= x - 6y + z - \frac{4y^3z^3}{(6y-z)(y+z)}, \\ G_4^{(3)} &= x - 7y + \frac{4y^2z^3}{7(y+z)}, \\ G_5^{(3)} &= x - 2z. \end{aligned}$$

ここで、$G_1^{(3)}$ と $G_3^{(3)}$ は共に分母因子 $6y-z$ を含む。さらに、$G_3^{(3)}$ と $G_4^{(3)}$ は共に分母因子 $y+z$ を含む。$G_1^{(3)}, G_3^{(3)}, G_4^{(3)}$ を以下の通りに組み合わせる。

$$G_1^{(3)}G_3^{(3)}G_4^{(3)} \equiv x^3 - 13x^2y + x^2z + 42xy^2 - 7xyz + 4y^3z^3.$$

$G_6^{(3)} = x^3 - 13x^2y + x^2z + 42xy^2 - 7xyz + 4y^3z^3$ とし、$\{G_2^{(3)}, G_5^{(3)}, G_6^{(3)}\}$ に拡張 *Hensel* 構成を適用する。4 次まで行うと以下の *Hensel* 因子を得る。

$$\begin{aligned} G_2^{(4)} &= x + 3y - \frac{3y^3z^3}{3y+2z}, \\ G_5^{(4)} &= x - 2z + \frac{3y^3z^3}{3y+2z}, \\ G_6^{(4)} &= x^3 - 13x^2y + x^2z + 42xy^2 - 7xyz + 4y^3z^3 - 8xy^3z^3. \end{aligned}$$

$G_2^{(4)}$ と $G_5^{(4)}$ は分母因子に $3y+2z$ を含む。これより、$G_2^{(4)}$ と $G_5^{(4)}$ を以下の通りに組み合わせる。

$$G_2^{(4)}G_5^{(4)} \equiv x^2 + 3xy - 2xz - 6yz + 3y^3z^3.$$

$G_7^{(4)} = x^2 + 3xy - 2xz - 6yz + 3y^3z^3$ とおくと、$G_6^{(4)}$ と $G_7^{(4)}$ は F で割り切れることから、これらが $\mathbf{Q}[x,y,z]$ 上の既約因子となる。 □

3.2 Newton 多角形の下辺の両側からの拡張 Hensel 構成

2 章において、$\mathcal{S}_1 \Rightarrow \mathcal{S}_2 \Rightarrow \cdots \Rightarrow \mathcal{S}_\rho$ ($\mathcal{S}_i$ $(i = 1, \ldots, \rho)$ は 定義 2 において定義されたもの) の順に Newton 多角形の下辺の右側から Newton 線とすることで、Hensel 因子を求めることができることを述べた。しかしながら、この方法で因数分解を行う為には拡張 Hensel 構成を高次まで計算する必要があり、計算時間が増える。そこで右側だけでなく、左側 ($\mathcal{S}_\rho \Rightarrow \mathcal{S}_{\rho-1} \Rightarrow \cdots \Rightarrow \mathcal{S}_1$) から Hensel 因子を求めることにより、高次の計算をせずに因数分解ができる。左側から Hensel 因子を求める際、$F(x,u)$ に変換 $\mathcal{T}_{\mathrm{Rev}}$ を施し、変換後の多項式に Hensel 構成を適用した後、逆変換 $\mathcal{T}_{\mathrm{Rev}}^{-1}$ を施すことにより Hensel 因子が得られる ([SI00] 参照)。

$$\mathcal{T}_{\mathrm{Rev}} : \ F(x,u) \ \mapsto \ x^{\deg(F)}F(1/x,u). \tag{6}$$

$\rho = 2$ の場合において説明する。まずは、拡張 Hensel 構成を右側から ($\mathcal{S}_1 \Rightarrow \mathcal{S}_2$) 行う。このとき

$$F(x,u) = G_0^{(\infty)}(x,u) \cdot G_1^{(\infty)}(x,u) \cdots G_\tau^{(\infty)}(x,u). \tag{7}$$

と分解される。次に拡張 Hensel 構成を左側から ($\mathcal{S}_2 \Rightarrow \mathcal{S}_1$) 行い、Hensel 因子を求めるが、まずは、$F(x,u)$ に (6) において記述された変換 $\mathcal{T}_{\mathrm{Rev}}$ を施す。$\tilde{F}(x,u) = \mathcal{T}_{\mathrm{Rev}}F$ とする。このとき $\tilde{F}(x,u)$ の Newton 線は $\mathcal{S}_2$ の他ならない。そして、Newton 多項式 $\tilde{F}_{\mathrm{New}}$ を以下の通りに $\mathbf{K}[x,u]$ 上で因数分解する。

$$\begin{cases} \tilde{F}_{\mathrm{New}}(x,u) = \tilde{H}_0(x,u) \cdot \tilde{H}_1(x,u) \cdots \tilde{H}_s(x,u), \\ \tilde{H}_0 = \mathrm{cont}(\tilde{F}_{\mathrm{New}})x^{n-n_0}, \quad \gcd(H_i, H_j) = 1 \ \ (\forall i \neq j). \end{cases} \tag{8}$$

もし、$s = 1$ ならば $G_0^{(\infty)}(x,u)$ は $F(x,u)$ の既約因子となり $\rho = 1$ の場合と同等になる。以下、$s \geq 2$ とする。

$\tilde{F}$ に拡張 Hensel 構成を適用することで以下を得る。

$$\tilde{F}(x,u) = \tilde{H}_0^{(\infty)}(x,u) \cdot \tilde{H}_1^{(\infty)}(x,u) \cdots \tilde{H}_s^{(\infty)}(x,u). \tag{9}$$

そして、$i=1,\ldots,s$ において $\bar{H}_i^{(\infty)} = \mathcal{T}_{\mathrm{Rev}}^{-1}\tilde{H}_i^{(\infty)}$ とする。[SI00] の Theorem 2 から次の対応が $\mathbf{K}\{(u)\}$ の単元の不定性を除いて得られる。

$$\{G_0^{(\infty)}\text{の Hensel 因子}\} \Longleftrightarrow \{\bar{H}_1^{(\infty)},\ldots,\bar{H}_s^{(\infty)}\},$$

実際の計算では、$\bar{H}_i^{(\infty)}$ $(i=1,\ldots,s)$ の主係数を $\mathrm{lc}(G_0^{(\infty)})$ に規格化することにより単元の不定性を除く。つまり $\mathrm{lc}(G_0^{(\infty)})/\mathrm{lc}(\bar{H}_i^{(\infty)})$ に $\bar{H}_i^{(\infty)}$ を掛ける。以上より規格化された Hensel 因子を $H_i^{(\infty)}$ $(i=1,\ldots,s)$ とすると、$\{G_1^{(\infty)},\ldots,G_r^{(\infty)},H_1^{(\infty)},\ldots,H_s^{(\infty)}\}$ を組み合わせることで $F(x,u)$ の因子を得る。

例 3

$$\begin{aligned}
F &= x^4(y^2-z^2)+x^3(y+3z+3y^2+3z^2)\\
&\quad + x^2(-2+3y-4z-2y^2+5yz-2z^2+y^3+6y^2z+3z^3)\\
&\quad + x^1(-5y-9y^2-5yz-5z^2+3y^3+y^2z-5z^3)\\
&\quad + (3y^2-5y^3-7y^2z-yz^2-2y^4-3y^2z^2-3yz^3-2z^4).
\end{aligned}$$

F の *Newton* 多角形は図 2 で示される。まずは $\mathcal{S}_1$ を *Newton* 線とする。このとき *Newton* 多項式 F_{New} の既約分解は以下の通りである。

$$F_{\mathrm{New}} = x^4(y^2-z^2)+x^3(y+3z)-2x^2 = x^2\cdot[x(y+z)-1]\cdot[x(y-z)+2].$$

$G_0=x^2$, $G_1=x(y+z)-1$, $G_2=x(y-z)+2$ とし、これらを初期因子として拡張 *Hensel* 構成を適用する。2 次まで行うと以下の *Hensel* 因子を得る。

$$\begin{aligned}
G_0^{(2)} &= x^2+x(5y/2+33y^2/4-5yz/2+5z^2/2)-3y^2/2,\\
G_1^{(2)} &= x(y+z)-1+2y-z-3y^2-3yz,\\
G_2^{(2)} &= x(y-z)+2+y+2z+y^2/2-yz/2.
\end{aligned}$$

次に $\mathcal{S}_2$ を *Newton* 線とする。F に *(6)* で記述された変換 $\mathcal{T}_{\mathrm{Rev}}$ を適用する。このとき、変換後の式 $\tilde{F}$ とその *Newton* 多項式 $\tilde{F}_{\mathrm{New}}$ は以下の通りになる。

$$\begin{aligned}
\tilde{F} &= x^4(3y^2-5y^3-7y^2z-yz^2-2y^4-3y^2z^2-3yz^3-2z^4)\\
&\quad + x^3(-5y-9y^2-5yz-5z^2+3y^3+y^2z-5z^3)\\
&\quad + x^2(-2+3y-4z-2y^2+5yz-2z^2+y^3+6y^2z+3z^3)\\
&\quad + x^1(y+3z+3y^2+3z^2)+(y^2-z^2),\\
\tilde{F}_{\mathrm{New}} &= 3x^4y^2-5x^3y-2x^2 = x^2\cdot(3xy+1)\cdot(xy-2).
\end{aligned}$$

$\tilde{H}_0=x^2$, $\tilde{H}_1=3xy+1$, $\tilde{H}_2=xy-2$ とし、これらを初期因子として拡張 *Hensel* 構成を適用する。2 次まで行い、それらの *Hensel* 因子 $\tilde{H}_i^{(2)}$ $(i=1,2)$ に逆変換 $\mathcal{T}_{\mathrm{Rev}}^{-1}$ を施す。その結果を $\bar{H}_i^{(2)} = \mathcal{T}_{\mathrm{Rev}}^{-1}\tilde{H}_i^{(2)}$ $(i=1,2)$ とすると以下を得る。

$$\begin{aligned}
\bar{H}_1^{(2)} &= x\,(1-2y+z+3y^2+3yz)+3y+y^2-yz+2z^2,\\
\bar{H}_2^{(2)} &= x\,(-2-y-2z-y^2/2+yz/2)+y-2y^2-2yz-z^2.
\end{aligned}$$

ここで $G_0^{(2)}$ の主係数は 1 だから、$\bar{H}_i^{(2)}$ $(i=1,2)$ の主係数を 1 に規格化することにより単元の不定性を除く。そこで $\bar{H}_i$ を $\mathrm{lc}(\bar{H}_j)$ で割る (べき級数除算) と以下を得る。

$$\begin{aligned}
H_1^{(2)} &\Leftarrow \bar{H}_1^{(2)}/\mathrm{lc}(\bar{H}_1^{(2)}) \equiv x+3y+7y^2-4yz+2z^2,\\
H_2^{(2)} &\Leftarrow \bar{H}_2^{(2)}/\mathrm{lc}(\bar{H}_2^{(2)}) \equiv x-y/2+z/2+5y^2/4+3yz/2.
\end{aligned}$$

以上により得られた *Hensel* 因子を組み合わせることにより F の既約因子を得る。実際、$G_i^{(2)}H_i^{(2)}$ $(i=1,2)$ は F を割る。

$$\begin{aligned}
G_1^{(2)}H_1^{(2)} &\equiv x^2y+x^2z+2xy-xz-x-y^2+yz-3y-2z^2,\\
G_2^{(2)}H_2^{(2)} &\equiv x^2y-x^2z+xy+2xz+2x+2y^2+2yz-y+z^2.
\end{aligned}$$

□

4 実験

本章では以下の3つの方法により、因数分解における効率性を実験により比較、検証する。1つは拡張 Hensel 構成を用いた方法、他の2つは従来の一般 Hensel 構成を用いた方法である。

- method H
  一般 Hensel 構成を用いて因数分解を行う。Hensel 構成が破綻する展開点に対しては多項式を平行移動させることにより展開点を変更する。また、主係数が定数でない場合、元の多項式を主係数でべき級数除算を行い、さらに各初期因子もそれぞれの主係数で割ることで、それら全ての主係数を 1 に規格化する。
- method W
  method H と同様に一般 Hensel 構成を用いて因数分解を行う。ただし、Wang の方法 [Wan77] を用いて Hensel 構成における各初期因子に対し適切に主係数を振り分ける。
- method E
  本稿で紹介した拡張 Hensel 構成を使用して因数分解を行う。

全ての実験において、変数が x, y, z (x が主係数) である3変数多項式を用いる。methods H, W に関して原点で y, z ともに非零代入を必要とするものとする。

実際の計算において Hensel 構成の次数を定める必要がある。method H, W では $\mathrm{tdeg}_{y,z}(F)/2$ 次、method E では Newton 多角形の下辺1本あたり、$\mathrm{tdeg}_{y,z}(\bar{F})/2$ 次ずつである。ただし、$\bar{F}$ は $F\times[G_0,\ldots,G_r$ に $\mathrm{lc}(F)$ の既約因子を振り分ける際に生じた $\mathrm{lc}(F)$ の既約因子の余剰分 ([Ina04], [Ina05] 参照)] である。

実験環境は以下の通りである。

OS	Linux 2.4.22
CPU	AMD Athlon(tm) XP 1900+ (1.60GHz)
Memory	1.00 Gbyte
Library	GAL(General Algebraic Language)

実験 1 非零代入による項の増大が顕著である例

以下の多項式を用いる。

$$\begin{aligned} P_k &= [\, x^2y^2z + x\,(y^k+z^k) + 3y + 3z - 3z^2 - 2y^{k/2}z^{k/2}\,] \\ &\times [\, x^3y^2z^2 + x\,(y^k+z^k) - 2y - 5z + 4y^2 + 3y^{k/2}z^{k/2}\,]. \end{aligned}$$

k が大きくなるほど P_k の従変数 y, z の全次数が大きくなり、非零代入による項の増大が大きくなる。この実験では k を $k=10\Rightarrow 20\Rightarrow\cdots\Rightarrow 50$ に増加して行った。実験結果を表1に記す。各表の T_H, T_W, T_E は methods H, W, E での平均計算時間である。また、右側2列の T_H/T_E, T_W/T_E はそれぞれ T_E に対する T_H, T_W の割合である。

k	T_H (sec)	T_W (sec)	T_E (sec)	T_H/T_E	T_W/T_E
10	0.0918	0.0240	0.0167	5.50	1.44
20	0.910	0.194	0.0319	28.5	6.08
30	5.66	0.823	0.0440	129.	18.7
40	21.6	2.61	0.0460	470.	56.7
50	63.6	6.23	0.0520	1220.	120.

表1：$P_{10}\sim P_{50}$ における平均計算時間

method E において、k が小さい内は他の2つの方法を比べてそれほど差は無いが、k が大きくなるほど、一般 Hensel 構成における非零代入の影響が大きくなる ($k=50$ では、非零代入での項の増加は約 250 倍以上になる) が、このとき、method E での効率性が明白になる。

実験 2 [Hensel 因子の個数] > [既約多項式因子の個数] である場合

以下の多項式を用いる。

$$\begin{aligned} Q_k &= [\,(x(\,y^3+2z^3)+5yz)(x\,(y+4z)+2)+(2x-7)\,(y^kz^k-y^{k-1}z^{k-1})\,] \\ &\times [\,(x\,(3y^3+4z^3)+3yz)(x\,(y+3z)+7)-(3x+5)\,(y^kz^k-y^{k-1}z^{k-1})\,]. \end{aligned}$$

この実験において、method H, W では展開点を $(y,z)=(1,1)$ とする。全ての方法において、Q_k の Hensel 因子は4個である。k を $k=5\Rightarrow 6\Rightarrow\cdots\Rightarrow 15$. に増加させて実験を行う。実験結果を表2に記す。

k	T_H (sec)	T_W (sec)	T_E (sec)	T_H/T_E	T_W/T_E
5	2.90	0.314	0.0984	29.5	3.19
6	5.99	0.784	0.106	56.5	7.40
7	11.2	1.73	0.115	97.4	15.0
8	20.4	3.51	0.124	165.	28.3
9	35.4	6.92	0.130	272.	53.2
10	58.7	12.7	0.137	428.	92.7
11	95.5	22.1	0.157	608.	141.
12	146.	36.2	0.166	880.	218.
13	221.	57.9	0.182	1210.	318.
14	329.	91.1	0.196	1680.	465.
15	473.	137.	0.219	2160.	626.

表 2：$Q_5 \sim Q_{15}$ における平均計算時間

表 2 によると、特に k が大きいとき、method E が他の 2 つと比べて非常によい効果をもたらすことが分かる。非零代入による Q_k の項の増大は 5~40 倍程度であるが、[Hensel 因子の個数] > [既約多項式因子の個数] の状況下では method H, W では k が増大するごとに計算時間が大幅に増大する。これに対して method E では 3.1 節で紹介した計算途中での有理式の組み合わせを行い、Hensel 因子の個数を減らすことにより、飛躍的に効率化されると考えられる。

実験 3

Newton 多角形の下辺が 2 本 (定義 2 において $\rho = 2$) である、4 個の既約多項式の積からなる 10 個の多項式 $H_1, \ldots, H_{10}$ を生成し、実験を行った。実験結果を表 3 に記す。生成した多項式における各因子は従変数 y, z について全次数が 40 以下で数係数が $\{-4, -3, \ldots, 3, 4\}$ のいずれかである項 3~8 項からなる多項式である。例を下に表す。

$$\begin{aligned} H_1 &= [\, x^2(-2+yz) - 3xy^{15}z^{14} + 3y^2 - z^2 - y^{15}z^6] \\ &\times [\, x^2yz + x\,(-3y^{13}z^{20} + 2y^{15}z^{14}) + 3 - 4yz^{12}] \\ &\times [\, x\,(-3+yz) + y + 3z] \\ &\times [\, x\,(y-3z) - 3]. \end{aligned}$$

	T_H (sec)	T_W (sec)	T_E (sec)	T_H/T_E	T_W/T_E
H_1	23.6	3.15	0.295	80.0	10.7
H_2	40.0	8.68	0.604	66.2	14.4
H_3	17.6	1.36	0.329	53.5	4.13
H_4	75.1	8.69	0.679	111.	12.8
H_5	69.1	3.43	0.457	151.	7.51
H_6	28.5	1.76	0.231	123.	7.62
H_7	378.	6.14	0.641	590.	9.58
H_8	16.9	4.83	0.690	24.5	7.00
H_9	46.5	5.95	0.511	91.0	11.6
H_{10}	222.	28.1	1.98	112.	14.2

表 3：$H_1 \sim H_{10}$ における平均計算時間

すべてのサンプルにおける非零代入による項の増大は 10~30 倍程度である。method E では拡張 Hensel 構成を各 $\mathrm{tdeg}_{y,z}(H_i)/2$ 次ずつ 2 回行った。表 3 より、どのサンプルにおいても method E がよい結果を得た。これは 3.2 節で紹介した方法を用い、method E の効率化をはかったことによるものであると考えられる。

5 まとめと課題

今回用いた拡張 Hensel 構成による因数分解法は一般 Hensel 構成を用いた方法と効率性という観点から比較すると、実験 1 において 非零代入における項数の増大の影響が大きいとき、計算時間の差がはっきりと現れた。実験 2 において [Hensel 因子の個数] > [既約多項式因子の個数] である場合の多項式について、絶大な効果が得られた。実験 3 において $\rho = 2$ である Newton 多角形を持つ多項式において効果が現れたことを実証した。しかし、今回用いた因数分解法は、まだ改良の余地がある。考えられる改良点を下記に記す。

1. 本稿では全ての従変数に対して同等の重みをつけたが、この重みを変更することにより、Newton 多角形や Newton 多項式が変化し、さらに効率化できる場合がある。

2. 本稿で用いた因数分解法は Newton 多項式が無平方でない場合には適用できない。[SK99] にはその場合について議論されているが、代数関数を導入する必要があり、実用化し難い。しかし、Iwami [Iwa03, Iwa04] により Newton 多項式が無平方でない場合に対して別の解決案が提案されており、そちらを利用した因数分解法も検討中である。

参 考 文 献

[GCL92] K. O. Geddes, S. R. Czapor and G. Labahn: Algorithms for computer algebra. Kluwer Academic Publishers, 1992.

[Ina04] 稲葉 大樹: 拡張 Hensel 構成を用いた多変数多項式の因数分解. 数理解析研究所講究録 1395, 2004

[Ina05] D. Inaba: Factorization of Multivariate Polynomials by Extended Hensel Construction. (ACM SIGSAM Bulletin, to appear)

[Iwa03] M. Iwami: Analytic factorization of the multivariate polynomial. *Proc. CASC'03 (Computer Algebra in Scientific Computing)*, Eds. V. G. Ganzha, E. W. Mayr and E. V. Vorozhtsov, 213-225 (2003).

[Iwa04] M. Iwami: Extension of expansion base algorithm to multivariate analytic factorization. *Proc. CASC'04 (Computer Algebra in Scientific Computing)*, Eds. V. G. Ganzha, E. W. Mayr and E. V. Vorozhtsov, 269-281 (2004).

[Kuo89] T.-C. Kuo: Generalized Newton-Puiseux theory and Hensel's lemma in $\mathbf{C}[[x, y]]$. Canad. J. Math., Vol. XLI, 1101-1116 (1989).

[SI00] T.Sasaki and D.Inaba: Hensel construction of $F(x, u_1, \ldots, u_l), l \geq 2$, at a singular point and its applications. ACM SIGSAM Bulletin, Vol.34, 2000, pp. 9-17

[SK99] T. Sasaki and F. Kako: Solving multivariate algebraic equation by Hensel construction. Japan J. Indus. Appl. Math., **16**, 257-285 (1999).

[Wan77] P. S. Wang: Preserving sparseness in multivariate polynomial factorization. *Proc. 1977 MACSYMA Users Conference*, MIT, 55-61 (1977).